UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/648,531	08/25/2003	Stuart Cain	200310063-1	4467

22879 7590 06/10/2008

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
ALMEIDA, DEVIN E	

ART UNIT	PAPER NUMBER
2132	

NOTIFICATION DATE	DELIVERY MODE
06/10/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/648,531
Filing Date: August 25, 2003
Appellant(s): CAIN, STUART

John P. Wagner Jr
Reg. No. 35,398
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 4/08/2008 appealing from the Office action mailed 12/11/2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows:

WITHDRAWN REJECTIONS

The following grounds of rejection are not presented for review on appeal because they have been withdrawn by the examiner. The rejection of claims 4, 5, and 9 have been withdrawn. The applicant argument with respect to the Fox not teaching that the asset value is an indication of the economic value of the functions provided by the network node has been fully considered and is persuasive.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6535227	Fox er al	3-2003
2002/0073338	Burrows et al.	6-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim 1-3, 6, 7, 10, 12-16, 19 and 20 are rejected under 35 U.S.C. 102(e) as being anticipated by Fox et al (U.S. 6,535,227). Fox teaches everything with respect to claim 1, a security indication spanning tree method comprising: determining asset value of a network node (see abstract and column 3 lines 34-59); ascertaining exposure rating of said network node (see abstract and column 3 lines 34-59); establishing a functional priority risk indicator for indicating the likelihood of an attack from another network node (see abstract and column 3 lines 34-59); and creating a spanning tree schematic of a network including said network node, wherein said spanning tree schematic includes an indication of said asset value (see abstract and figure 7, 9 and 10).

With respect to claim 2, wherein said spanning tree schematic includes an indication of said exposure rating (see abstract and figure 7, 9 and 10).

With respect to claim 3, wherein said spanning tree schematic includes an indication of said attack risk (see column 1 lines 31-58).

With respect to claim 6, a security indication spanning tree method of claim 1 wherein said exposure rating defines a threshold value corresponding to connectivity of

the network node with other network nodes (see abstract and figure 7, 9 and 10 and column 9 line 20-25).

With respect to claim 7, wherein said network node is given an exposure rating value based upon a connectivity distance from a root node (see column 9 lines 20-25).

With respect to claim 8, wherein said root node is a node closest to an external network (see figure 1).

With respect to claim 10, a security indication spanning tree system comprising: a bus for communicating information; a processor coupled to said bus (see column 5 lines 35 –51 it is inherent that a computer has a processor), said processor for processing said information including instructions for building an attack impact susceptibility spanning tree representation including asset value factors (see column 5 lines 35 -51); and a memory coupled to said bus, said memory for storing said information (see column 5 lines 35 –51 it is inherent that a computer has a memory), including instructions for building said attack impact susceptibility spanning tree representation including said asset value factors (see abstract, figure 7, 9 and 10 and column 3 lines 34-59).

With respect to claim 11, wherein said asset risk value is automatically determined (see column 5 lines 35 -51).

With respect to claim 12, further comprising a central console for interfacing with a network application management platform (see Abstract and column 5 lines 35 –51).

With respect to claim 13, wherein said instructions include attack spread risk determination instructions (see column 1 lines 31-58).

With respect to claim 14, wherein said instructions include exposure rating determination directions (see figure 3 and column 5 lines 35 – column 6 lines 51 and column 7 line 28 – column 8 line 6).

With respect to claim 15, a computer usable storage medium having computer readable program code embodied therein for causing a computer system to implement security indication spanning tree instructions comprising: a device examination module for examining information regarding devices included in a centralized resource network, wherein said examining includes ascertaining what applications said devices support; an importance indication module for obtaining an indication of a relative importance of functionality provided by said device (see column 5 lines 35 –51 and column 7 line 28 – column 8 line 6); and a spanning tree module for building a spanning tree topology representation including said indication of said relative importance of said device in supporting said applications (see abstract, figure 7, 9 and 10 and column 3 lines 34-59).

With respect to claim 16, herein said relative importance of said device is based upon an economic value of functions said devices performs in support of said applications (see column 1 lines 31-58).

With respect to claim 19, further comprising an attack danger assessment module for assessing the danger of an attack from other devices included in said network (see column 1 lines 31-58).

With respect to claim 20, further comprising: deriving an attack danger indication based upon said indication of said relative importance of said device and said

connectivity threshold value; and associating said attack danger indication with said device (see column 1 lines 31-58).

Claim Rejections - 35 USC § 103

Claims 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fox et al (U.S. 6,535,227) in view of Burrows et al (U.S. 2002/0073338). Fox teaches everything with respect to claim 15 but with respect to claim 17 Fox does not teach further comprising an internal attack permeability module for investigating the permeability of a network in permitting an internal attack on a device from other devices included in the network. 17. Burrows an internal attack permeability module for investigating the permeability of a network in permitting an internal attack on a device from other devices included in the network (see Borrows paragraph 0040-0041). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Fox with the method of Burrows to diffuse attack from a first component to a second component in the network in order to mitigate the effects of undesirable behavior on the network, as taught by Burrows (see Burrows paragraph 0028]).

With respect to claim 18 wherein said investigating includes: analyzing the ease of attack on said device from other devices in said centralized resource network; and assigning an connectivity threshold value to said device based upon said analysis of said ease of attack (see Borrows paragraph 0040-0041).

(10) Response to Argument

Applicant's arguments with respect to claim 1 have been fully considered but they are not persuasive. Fox clearly teaches "determining asset value of a network node" and "creating a spanning tree schematic of a network including said network node, wherein said spanning tree schematic includes an indication of said asset value" in column 3 lines 34-59 i.e. "network elements determine different color indicative of a vulnerable network element. A graphical user interface can also comprise a manager window for displaying properties of network elements. A data sensitivity box can have user selected items for selecting the sensitivity of network elements. The graphical user interface can also comprise a select node configuration edit box having a user selectable vulnerability profile for selecting a vulnerability profile of a network node. The icons can be linked together by arrows that turn a different color indicative of a vulnerable connection that exists between those work elements... a graphical user interface is contained on a computer screen and used for determining the vulnerability posture of a network. It includes a system design window for displaying icons of a network map that are representative of different network nodes contained within a network. The respective icons are linked together in an arrangement corresponding to how network nodes are interconnected within the network. A manager window an be included and respective properties of network nodes can be displayed and edited. The selected icons turn the color red indicative of a higher risk node, and selected icons turn yellow indicative of a less severe risk node after a vulnerability posture of the network has been established."

The colors represent different asset values with red being higher risk node and yellow indicative of a less severe risk node.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., that the asset value is an indication of the economic value of the network node) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Claim 1 is broader then the applicant is arguing. The asset value can be any vulnerability or security and does not have to be an economic value of the network node to meet the limitations of the claims.

Applicant's arguments with respect to claims 17 and 18 have been fully considered but they are not persuasive. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the method of Burrows could be used to diffuse attack from a first component to a second component in the network in order to mitigate the effects of undesirable behavior on the network. The combination of Fox's vulnerability posture

with Burrows method of limiting the impact of undesirable behavior with allow the Fox system to fine vulnerability in a system and limit the impact of the of the vulnerability on the network system.

For the above reasons, it is believed that the rejections should be sustained.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

Respectfully submitted,

/Devin Almeida/
Examiner, Art Unit 2132

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132

Conferees:

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132